City of Gillette		Administrative Policy/Procedures (APP)
Number: 4.1		*Subject:* Information Technology Acceptable Use Policy
Original Issue: 2-9-04	*Effective: 2-9-04*	
Current Issue: 2-9-04	*Effective: 2-9-04*	*Category:* Information Technology Services
Supersedes: n/a		

Access to the computer systems and networks owned and/or operated by the City of Gillette, including personal digital assistants, telemetry systems, and personal use communication systems, imposes certain responsibilities upon users, in accordance with City policy and local, state and federal law. These policies do not apply to Police Department personnel in the conduct of their investigative duties however they must still follow Police Department policies governing the same. Users accept the responsibility for utilizing services in ways that are ethical, demonstrates integrity and maintains respect for others who share this resource. This policy is established in an effort to help users understand what is expected of them in their use of City-provided technology. It sets guidelines regarding the issues of privacy and respect for property, ownership of data, system security, and gives definition to those applications of technology that the City considers misuse of the system.

The City reserves the right to amend, clarify, expand or append this policy as needed in the future. Such changes shall be distributed to all users and will become a part of this policy without the execution of a second acknowledgement form.

A. A Shared Resource

Because there are so many individuals who utilize this shared resource, respect for the confidentiality needs of the City are central to this policy. To ensure access and service for all users, users must refrain from any action, which interferes with the system, such as:

1. Using computer or network services for commercial or personal purposes.

2. Knowingly installing or running a program that will damage or place an undue burden on the system.

3. Tampering with or trying to circumvent security systems.

4. Knowingly acting in a manner that will disrupt normal operations of computers or the network.

5. Intentionally or repeatedly obstructing City work by consuming large amounts of system resources (disk space, CPU time, print quotas, network bandwidth) or by deliberately crashing the machine(s) may result in loss of system privileges or other forms of disciplinary action.

B. Privacy

Although there can be no expectation of absolute privacy in the use of City computers and technology, technology should not be used in a manner that infringes upon the necessary confidentiality of City matters. The following restrictions are imposed to protect confidentiality of City matters. Unless authorized to do so, users are *prohibited* from:

1. Using computer or network services in a way that violates copyrights, trademarks, patent protections or license agreements.

2. Gaining unauthorized access to information that is confidential or protected, or attempting to do so.

3. Running programs that attempt to identify passwords or codes.

4. Interrupting programs that protect data or secure systems, or attempting to do so.

5. Monitoring or tampering with another person's e-mail.

6. Reading, copying, changing or deleting another person's work.

7. Using another person's password, or allowing others to use yours.

8. Attempting to gain network privileges to which the user is not entitled.

C. Appropriate Exchange of Ideas and Information

Computer systems and networks allow for a free exchange of ideas and information. This exchange serves to enhance learning, teaching, critical thinking and research. City Employees should be aware that City policy and local, state and federal law *prohibit* some forms of communications, including but not limited to:

1. Obscenity.

2. Defamation.

3. Advocacy directed to incite or produce lawless action.

4. Threats of violence.

5. Disruption of the business environment.

6. Harassment based on sex, race, disability or other protected status.

7. Anonymous or repeated messages designed to annoy, abuse or torment.

8. Overuse of interactive network utilities, etc..

D. Personal Responsibility

Each individual who obtains a computer/e-mail account, or uses the computers and network resources made available by the City of Gillette, must understand that he/she is accountable for complying with the policies set forth in this document. In addition, users assume responsibility for:

1. Protection of his/her password.

2. Reporting any breach of system security.

3. Reporting unauthorized use of his/her account.

E. Authority

The Information Technology Manager or his/her designee may access other's files for the maintenance of networks, computers and storage systems. In all cases, all confidential City communications will be protected. Log usage data, such as network connection times, CPU and disk utilization for each user, security audit trails and network loading may also be routinely monitored. Data collected may be reviewed and further investigated as necessary to insure compliance with City policy and all laws. If necessary, the Information Technology Manager or his/her designee, with authorization from the City Administrator, may monitor the activities and files of specific users on their computers and networks. In the event the user in question utilizes a machine in the Police Department, the IT Manager shall inform the Chief of Police in advance of such monitoring activity. The computer aided dispatch stations within the Police Department shall not be monitored due to sensitive data and all inquiries associated with these machines shall be directed to the Chief of Police. Any Information Technology employee who believes such monitoring is necessary should discuss the problem and strategy for investigation with the Information Technology Manager prior to conducting monitoring.

The Information Technology Manager or his/her designee may periodically monitor the use of computer hard drives, network access records, internet access records, data log information and other aspects of computer operations as a part of the responsibilities of their position.